

## REMARKS

No claims have been added, canceled or amended. Claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50, 52-54 are still pending in this application.

The independent claims 1, 25, 37 and 52 had been rejected under 35 USC §103 as being unpatentable over *Carrott et al.* (*Carrott*) in view of *Tsuei et al.* (*Tsuei*).

As discussed in the previous reply -- on page 11 of Reply D, although not enumerated as “a)” and “b)” -- each independent claim requires:

a) an enrollment process in which a trusted party verifies the identity of the presenter using the enrollment data; and

b) then associating authentication data (for example, a password) with the presenter; and the trusted party also communicates the password to the presenter (or vice versa); the password is secret in that it is known only to the trusted party and to the presenter.

In the portion of the Office Action entitled “Response to Arguments,” the Examiner focused on b), discussing where it is contended that “Tsuei discloses assigning passwords (paragraphs 104-139, 164,188) by a user to authenticate access and transactions via a trusted party.

In this present Reply E, Applicant would like to once again focus on a) – wherein during an enrollment process, a trusted party verifies the identity of the presenter using the enrollment data. The Examiner explicitly recognizes that Carrott, the primary reference, does not disclose a). In particular, the Examiner states in the paragraph of the Office Action bridging pages 3 and 4 (emphasis added):

Carrott does not explicitly disclose receiving by said trusted party [during] and enrollment process, profile data and enrollment data from said presenter and verifying the identity of said presenter, said trusted party being an issuer of an account to said presenter wherein authentication data is received and validated as per the customer profile during an online transaction.

We therefore look for any statement by the Examiner that Tsuei, the secondary reference, discloses a) – namely an enrollment process in which a trusted party verifies the identity of the presenter using the enrollment data.

The Examiner’s contentions with respect to Tsuei, however, utterly fail to even discuss any contention of where Tsuei allegedly discloses an enrollment process in which a trusted party

verifies the identity of the presenter using the enrollment data. Rather, the Examiner's contentions with respect to Tsuei are for what Tsuei allegedly discloses relative to transactions that occur *after* an enrollment process. The Examiner makes no contentions about what occurs *during* an enrollment process.

In particular, to emphasize once again, the claims require an enrollment process in which a trusted party verifies the identity of the presenter using the enrollment data. The advantage of the enrollment process is that the trusted party verifies the presenter (and, therefore, the associated profile data) such that the trusted party can later authenticate that any profile data submitted by the presenter to a merchant (an "acceptor") during a later transaction is authentic. The password (or other authentication data) established during the enrollment process is later used by the presenter to prove that he is who he says he is (i.e., that he is the same person whose identity was verified during the enrollment process).

In Reply D, Applicant discussed in some detail why the "true identity" mentioned by Tsuei is merely the assumed "true identity" and is not a verified true identity as required by item a) of Applicant's claims. More specifically, Applicant discussed that Tsuei's central data base repository holds customer information, and the database is used to compare this information against third-party requests and thus verify the accuracy of the third party requests. However, as Applicant previously pointed out, if the customer information in the central database is not correct to begin with, there can be no authentication. Again, the Examiner makes no contention about Tsuei verifying the identity of the presenter using the enrollment data. Furthermore, as Applicant has amply demonstrated, Tsuei in fact has no such disclosure.

For example, referring again to the Reply D, Applicant discussed that the Tsuei discussion of Paragraph 14 merely discloses authenticating customer information in the central database for a third party asking for the information. However, the customer information in the central database was provided by the "customer," and there is nothing in Tsuei that discloses verifying the identity of the presenter of such information, at enrollment time. Put another way, even if the presenter of the information was an imposter, as a result of the enrollment process, the imposter would be able to carry out transactions with respect to such information. In accordance with the subject matter recited in the independent claims, on the other hand, such information never would have made it into a central database since it would have been determined that the presenter of the information was an imposter during the process of attempting to verify the identity of the presenter.

To recap, the Examiner has explicitly stated that the primary reference to Carrott does not disclose verifying the identity of the presenter of enrollment information. Furthermore, while the Examiner has summarily stated that Tsuei discloses such a feature, the Examiner has not pointed out where Tsuei is contended to disclose the feature. Finally, Applicant has amply demonstrated that Tsuei, in fact, does not disclose the feature.

The above discussion is applicable to all of the presently-pending claims.

Consideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at 408-255-8001.

Respectfully submitted,  
BEYER WEAVER LLP

/ASH/  
Alan S. Hodes  
Reg. No. 38,185

P.O. Box 70250  
Oakland, CA 94612-0250  
(408) 255-8001